

## DATA MANAGEMENT CARD

**Publication number:** JP2001077806

**Publication date:** 2001-03-23

**Inventor:** KASHIWA HIROSHI

**Applicant:** MATSUSHITA ELECTRIC IND CO LTD

**Classification:**

- international: **G06K19/00; G06F15/00; G06F21/00; H04L9/14; H04L9/32; H04N7/16; G06K19/00; G06F15/00; G06F21/00; H04L9/14; H04L9/32; H04N7/16; (IPC1-7): H04L9/14; G06F15/00; H04L9/32; H04N7/16**

- European:

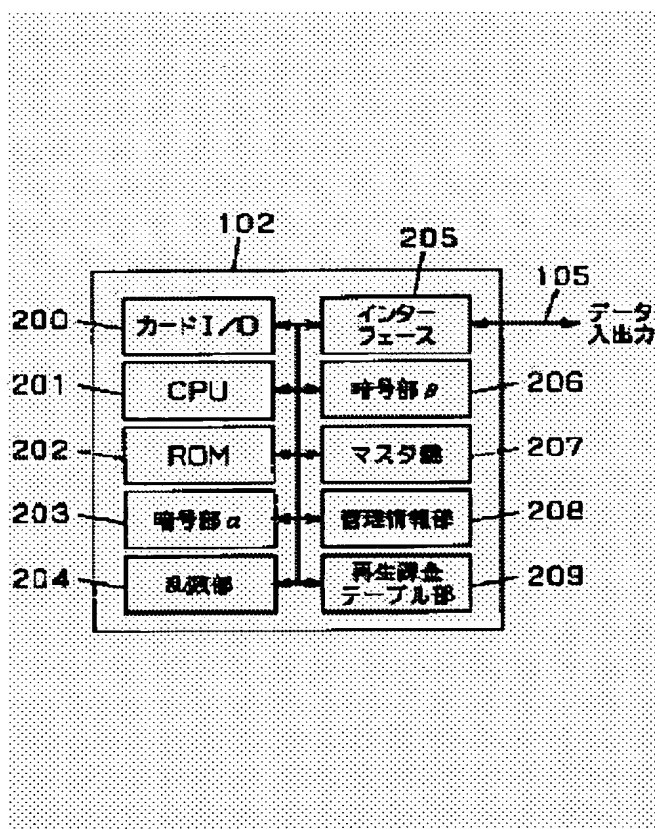
**Application number:** JP19990248350 19990902

**Priority number(s):** JP19990248350 19990902

Report a data error here

### Abstract of JP2001077806

**PROBLEM TO BE SOLVED:** To ensure a copyright protection function of contents recorded in a medium and to secure security required for it by using a card provided with an interface. **SOLUTION:** A card 102 has different encryption algorithm sets (encryption sections  $\alpha$ ,  $\beta$ ), the encryption section  $\alpha$  203 decodes contents that are encrypted and transmitted, the encryption section  $\beta$  206 is used at recording, the contents that are encrypted by using a random number for a key and an identification code using the random number are recorded in a medium, the card has the identification code by each title of the contents and the decoding key, the identification code is used at reproduction of contents, key information not open to public is decoded at an outside of the card so as to attain copyright management such as output of contents to other recorder without recording the copyright protection information like the decoding key to the medium.



Data supplied from the esp@cenet database - Worldwide

[0033]

(Recoding content on media)

The following will explain an operation for recording contents from a broadcast source station 100 to a reception, recording and reproducing apparatus 101. FIG. 4 shows a configuration view of a card 102.

[0034]

In FIG. 4, 200 denotes a card I/O for performing data transmission and reception with the reception, recording and reproducing apparatus 101, 201 denotes a CPU that controls the card 102, 202 denotes a ROM that stores a program executed by the CPU 201, 203 is an encryption section  $\alpha$  having cryptographic algorithm for use in content to be distributed from the broadcast source station 100, 204 denotes a random number generator, 205 denotes an interface that performs data transmission and reception with an outer device of the reception, recording and reproducing apparatus 101, 206 denotes an encryption section  $\beta$  having cryptographic algorithm for use in recording distributed content on media and the like, 207 denotes a master key that is a key for decoding encrypted content distributed from the broadcast source station, 208 denotes a management information section that is configured by an involatile memory that stores information necessary for reproducing content, and 209 denotes a reproduction charging table section that is configured by an involatile memory to be used in processing reproduction charging to be described later.

[0035]

FIG. 5 is a configuration view of the reception, recording and reproducing apparatus 101. In FIG. 5, 210 denotes a network interface for performing data transmission and reception with the broadcast source station 100 through a public network 103, 211 denotes an expansion processing section that decodes data of MPEG video and audio, 212 denotes a card I/O for performing data transmission and reception with card 102, 213 denotes a signal processing section that creates a recording format, 214 denotes a laser drive section, 215 denotes an optical head section, 216 denotes a disk, 217 denotes a CPU that controls the reception, recording and reproducing apparatus 101, and 218 denotes a setting section 218 that sets an operation of the reception, recording and reproducing apparatus 101 by a user. [0036]

Here, the card 102 is installed in the reception apparatus 101 so as to allow communications using the card I/O 200 and the card I/O 211 of the reception, recording and reproducing apparatus 101. [0037]

Table 1 shows a format of storage data in the management information section 208, 300 denotes a content title, 301 denotes an identification code for performing identification for each content, 302 denotes a key to be used when the content is encrypted and recorded, 303 denotes a copy number restriction code for restricting the number of times when the content is output to an outer section, 304 denotes a class code for identifying a rate for reproduction charge when recording on

the medium is performed for each content, 305 denotes a date code indicating date when recording is performed for each content, 306 denotes a reproduction restriction code for restricting quality of the content recorded on the medium when  
5 outputting it to the outer section of the reproduction apparatus, 307 denotes a trace code for recording a distribution source for each content when the content is recorded, and 308 denotes a charging rate when reproduction charging is carried out.

[0038]

10 [Table 1]

				REPRODUCTION CHARGING SECTION				
TITLE 300	IDENTIF ICATION CODE 301	KEY 302	COPY NUMBER RESTRICTION CODE 303	CLASS CODE 304	DATE CODE 305	REPRODUCTION RESTRICTION CODE 306	TRACE CODE 307	CHARGING RATE 308
X	B	A	2	T1	1999.4	011		
.	.	.	.					
.	.	.	.					

[0039]

The following will explain an operation for recording a  
15 content of a title X to the reception, recording and reproducing apparatus 101. First, the content transmitted in an encrypted format from the broadcast source station 100 via the network 103 is received by the network interface 210 of the reception,

recording and reproducing apparatus 101 and is transmitted to the card 102 through the card I/O 212.

[0040]

In the card 102, a control program of the ROM 202 is executed by the CPU 201, whereby the random number generator 204 generates a first random number to serve as a key A in step S11 as shown in FIG. 6. In step S12, the random number generator 204 generates a second random number to serve as a random number A. In step S13, the random number A is compared with information registered as an identification code in the management information section 208. When a match is found (No), step S12 is executed, and when no match is found (Yes), the random number A is used as an identification code B in step S14. This creates a pair of identification codes that can distinguish between a key for encrypting content at a recording time to be described later and a key that is stored in the card 102 necessary for decoding the content at a reproducing time.

[0041]

Then, the content input through the card I/O 200 is decoded in a predetermined unit by the encryption  $\alpha$  203 using the master key 207, the content is encrypted by the encryption section  $\beta$  206 using the key A, and the identification code B and the encrypted content are transmitted to the reception, recording and reproducing apparatus 101 from the card I/O 200. Furthermore, the key A, identification code B and information, which is specifically described later and which is included in the header information section 117, are stored in the management

information section 208 on a title basis as shown in table 1.  
If no setting is made here, zero is set and the explanation is  
given as follows.

[0042]

5           The reception, recording and reproducing apparatus 101  
converts the identification code and the content received by  
the card I/O 212 to a recording format after an error correction  
code for correcting an error is added by the signal processing  
section 213, and processing for converting the recorded  
10 information from an electrical signal to an optical signal is  
carried out by the laser drive section 214, and the result is  
recorded on the disc 216 by the optical head section 215.

[0043]

          The cryptographic algorithm for use in distributing the  
15 content via the network is made different from the cryptographic  
algorithm for use in the media recordable or reproducible device  
by the aforementioned operation, whereby even if the  
cryptographic algorithm for use in the network is decoded, it  
is impossible to decode the content, which has been encrypted  
20 and recorded on the media, and this strengthen the safety of  
content copyright protection.

[0044]

          Moreover, by converting the encryption of content in the  
card, it is possible to perform conversion of encryption as the  
25 security of content is maintained without making a plaintext,  
which is in the process of being converted, open to the public.

[Brief Description of the Drawings]

[FIG. 1] A configuration view of a transmission system according to one embodiment of the present invention;

[FIG. 2] A block diagram showing a content encryption transmission configuration in the same transmission system;

5 [FIG. 3] A transmission format confirmation view of the same transmission system;

[FIG. 4] A configuration view of a card used in the same transmission system; and

[FIG. 5] A configuration view of a reception, recording  
10 and reproducing apparatus of the same transmission system.

[FIG. 1]

RECEIVING SIDE

PUBLIC

TRANSMITTING SIDE

5 100: BROADCAST SOURCE STATION

[FIG. 2]

RECEIVING SIDE

110: DECODING

10 111: MASTER KEY

112: CONTENT KEY

CONTENT

PUBLIC

TRANSMITTING SIDE

15 109: MASTER KEY

108: CONTENT KEY

107: ENCRYPTING

CONTENT

20 [FIG. 3]

113: PREAMBLE

114: TRANSMISSION DESTINATION ADDRESS

115: TRANSMISSION SOURCE ADDRESS

116: DATA SECTION

25 117: HEADER INFORMATION SECTION

118: DECODING KEY INFORMATION SECTION

119: CONTENT INFORMATION SECTION



[FIG. 4]

200: CARD I/O

203: ENCRYPTION SECTION A

5 204: RANDOM NUMBER SECTION

205: INTERFACE

206: ENCRYPTION SECTION B

207: MASTER KEY

208: MANAGEMENT INFORMATION SECTION

10 209: REPRODUCTION CHARGING TABLE SECTION

DATA INPUT/OUTPUT

[FIG. 5]

210: NETWORK INTERFACE

15 211: EXPANSION PROCESSING SECTION

212: CARD I/O

213: SIGNAL PROCESSING SECTION

218: SETTING SECTION

214: LASER DRIVE

20 DATA INPUT/OUTPUT

VIDEO OUTPUT

AUDIO OUTPUT

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2001-77806  
(P2001-77806A)

(43)公開日 平成13年3月23日(2001.3.23)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1 5 B 0 3 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
G 0 6 K 19/00		H 0 4 N 7/16	Z 5 C 0 6 4
H 0 4 L 9/32		G 0 6 K 19/00	Q 5 J 1 0 4
H 0 4 N 7/16		H 0 4 L 9/00	6 7 3 E

審査請求 未請求 請求項の数9 OL (全11頁)

(21)出願番号 特願平11-248350

(22)出願日 平成11年9月2日(1999.9.2)

(71)出願人 000005821

松下電器産業株式会社  
大阪府門真市大字門真1006番地

(72)発明者 柏 浩

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74)代理人 100097445

弁理士 岩橋 文雄 (外2名)

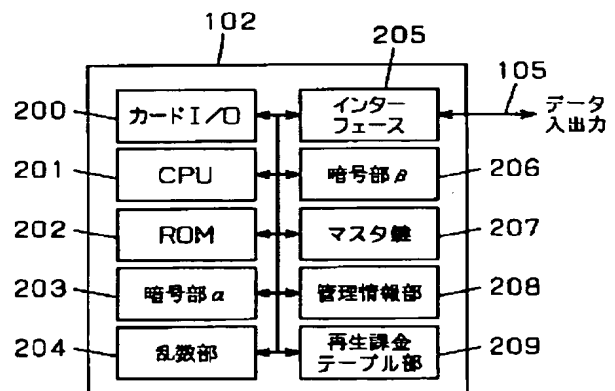
最終頁に続く

(54)【発明の名称】 データ管理カード

(57)【要約】

【課題】 インターフェースを備えたカードを用い、メディアに記録したコンテンツの著作権保護機能とそれに必要なセキュリティを確保する。

【解決手段】 異なる暗号アルゴリズム(暗号部 $\alpha$ 、 $\beta$ )をカード102に有し、暗号部 $\alpha$ 203で暗号化され伝送されてくるコンテンツを復号し、記録時は暗号部 $\beta$ 206を用い、乱数を鍵として暗号化したコンテンツと乱数を用いた識別コードをメディアに記録し、カードにコンテンツのタイトル毎に識別コードと復号鍵を有し、コンテンツ再生時に識別コードを利用し、カード外部に鍵情報を未公開で復号化することで、復号鍵等の著作権保護情報をメディアに記録することなくコンテンツを他の記録装置への出力などの著作権管理をも可能とする。



**【特許請求の範囲】**

【請求項 1】メディアへの記録または再生する機能を備えた装置と通信することでコンテンツの管理を行うための 2 種類以上の暗号アルゴリズムと、外部装置との通信を目的とするインターフェースを少なくとも有し、前記メディアに記録するデータに用いる暗号アルゴリズムと前記インターフェースで通信に用いる暗号アルゴリズムが異なることを特徴とするデータ管理カード。

【請求項 2】乱数を発生する乱数発生器をさらに備え、前記メディアにコンテンツを暗号化して記録する場合、前記乱数発生器を用いて記録するコンテンツ単位（名）で暗号化するための鍵を作成し、記録するデータ単位（名）毎に異なる様に前記乱数発生器を用いて独特の識別コード情報を作成し、該カードと前記メディアに同一の識別コードを記憶することを特徴とする請求項 1 記載のデータ管理カード。

【請求項 3】メディアに記録されているコンテンツのインターフェースから外部装置への出力を制限する複写回数制限コード情報を記憶し、前記複写回数制限コードを有するコンテンツを出力する場合にコンテンツ毎に複写回数制限コードを更新し所定値になることで外部への出力を不可能とすることを特徴とする請求項 1 記載のデータ管理カード。

【請求項 4】メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金を行うために、コンテンツ毎に料金識別するための等級コードの情報と、日付を示す日付コードの情報と、前記日付コードにより前記等級コードを選択するための転送コードの情報を有し、前記ディスクへの記録時にコンテンツ毎に前記等級コードと前記日付コードを記憶し、再生時において前記等級コードより選択される料金を加算することを特徴とする請求項 1 記載のデータ管理カード。

【請求項 5】メディアにインターフェースを介してコンテンツを記録する場合、該コンテンツの発信源を識別可能なトレースコードの情報を記憶することを特徴とする請求項 1 記載のデータ管理カード。

【請求項 6】コンテンツの視聴の条件を制約する再生制約コードの情報を付加されたコンテンツをメディアに記録または再生する場合、記録時に再生制約コードを記憶し、再生時にコンテンツの再生制約コードに応じた制約になるように記録または再生の制御を行うことを特徴とする請求項 1 記載のデータ管理カード。

【請求項 7】異なる暗号アルゴリズムである第 1 暗号部と第 2 暗号部を有するカードを用い、前記第 1 暗号部で暗号されて伝送されてくる情報を復号し、情報をメディアに記録する場合は第 2 暗号部を用いて暗号化することを特徴とするデータ管理方法。

【請求項 8】乱数を鍵として暗号化したコンテンツと乱数を用いた独特の識別コードをメディアに記録することを特徴とする請求項 7 記載のデータ管理方法。

【請求項 9】カードにコンテンツのタイトル毎に識別コードと復号鍵を持たせ、コンテンツを再生する場合に前記識別コードを用いて、前記カード外部に鍵情報を公開することなく復号化することを特徴とする請求項 7 記載のデータ管理方法。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、メディア記録されたコンテンツの再生に必要な情報を、カードを用いて管理するシステムに用いられるデータ管理カードに関するものである。

**【0002】**

【従来の技術】有線テレビジョン放送などでは、情報発信側である放送局と受信側との間で結ばれた契約内容に応じて、契約者になったユーザに発信される。具体的にはビデオ、オーディオ等のコンテンツを発信側が著作権保護するために暗号化し、受信契約を結んだユーザに IC カードを発行し、契約者のみに復号化を可能にする限定受信システムが導入されている。

【0003】この限定受信システムでは、契約者側の IC カードが備えられた受信装置で放送局側から暗号化されて配信されたコンテンツを復号して視聴する。

**【0004】**

【発明が解決しようとする課題】しかしながら、上記従来の構成では、発信側から伝送されたコンテンツをメディアに記録する場合に、記録したいコンテンツを暗号化したままで記録し、再生時に復号することが考えられるが、発信の暗号方式が解読された場合に、メディアに暗号化して記録しているコンテンツを自由に復号化することが可能であり、著作権保護の観点で問題を有していた。

【0005】また、コンテンツを復号するための鍵を暗号化してメディアに配置したとしても、例えばディスク系、テープ系にしる、メディアを再生できる装置であれば記録データを容易に取得可能であり、解読の危険性と言う点で問題を有していた。

【0006】また、著作権保護の観点から、コンテンツメーカの要望として以下（1）～（4）が求められている。

【0007】（1）メディアに記録されたコンテンツを別の装置（メディア）に出力する場合に、その回数を制限する。

【0008】（2）メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金。

【0009】（3）メディアにコンテンツを記録する場合に、不正なコンテンツの流通を防止するために、コンテンツの発信源を識別可能な情報の保持。

【0010】（4）メディアに記録されたコンテンツを別の装置（メディア）に出力する場合に、そのコンテンツの視聴の条件を制約する。

【0011】上記要望を実行する方法としては、各制御情報をコンテンツと共にメディアに記録することで行うことが考えられるが、前記理由により適切ではなく、メディアへの記録または再生可能な装置自身に保持する方法もあるが、装置を制御するCPUのプログラムへの改竄による不正行為が考えられる。

【0012】そのため、メディアでもなく、装置でもないセキュリティ機能を有する著作権保護を行う第3者の存在が望まれる。

【0013】本発明は、上記従来の問題点を解決するためになされたものであり、メディアへの記録または再生可能な装置にインターフェースを内蔵した取り外し可能でセキュリティ機能を付加可能なカードを用いて上記(1)～(4)および下記(5)、(6)の機能を提供することを目的とする。

【0014】(5)インターフェースを介した通信とメディアのコンテンツに用いる暗号アルゴリズムが異なる様に機能する。

【0015】(6)メディアに暗号化したコンテンツを記録した場合に、コンテンツを復号化する鍵をメディアに記録することなく復号可能である。

【0016】

【課題を解決するための手段】本発明は上記目的を達成するために、第1発明に係わるデータ管理カードは、メディアへの記録または再生する装置と通信することでコンテンツの管理を行うために2種類以上の暗号アルゴリズムと、外部装置との通信を目的とするインターフェースを少なくとも有し、メディアに記録するデータに用いる暗号アルゴリズムとインターフェースで通信に用いる暗号アルゴリズムが異なる様に変換することを備えた構成を有する。

【0017】第2発明に係わるデータ管理カードは、メディアにコンテンツを暗号化して記録する場合において、乱数を発生する乱数発生器を備え、乱数発生器を用いて記録するコンテンツ単位(名)で暗号化するための鍵を作成し、記録するデータ単位(名)毎に異なる様に乱数発生器を用いて独特の識別コードの情報を作成し、該カードとメディアに同一識別コードを記憶することを備えた構成を有する。

【0018】第3発明に係わるデータ管理カードは、メディアに記録されているコンテンツのインターフェースから外部装置への出力を制限する複写回数制限コードの情報を記憶し、記録回数制限コードを有するコンテンツを出力する場合にコンテンツ毎に複写回数制限コードを更新し、所定値になることで外部への出力を不可能とすることを備えた構成を有する。

【0019】第4発明に係わるデータ管理カードは、メディアに記録したコンテンツを再生する毎に料金を徴収するための再生課金に際し、コンテンツ毎に料金識別するための等級コードの情報と、日付を示す日付コードの

情報と、日付コードにより等級コードを選択するための転送コードの情報を有し、ディスクへの記録時にコンテンツ毎に等級コードと前記日付コードを記憶し、再生時において等級コードより選択される料金を加算することを備えた構成を有する。

【0020】第5発明に係わるデータ管理カードは、メディアにインターフェースを介してコンテンツを記録する場合、該コンテンツの発信源を識別可能なトレースコードの情報を記憶することを備えた構成を有する。

【0021】第6発明に係わるデータ管理カードは、コンテンツの視聴の条件を制約する再生制約コードの情報を付加されたコンテンツをメディアに記録または再生する場合、記録時に再生制約コードを記憶し、再生時にコンテンツの再生制約コードに応じた制約になるように前記記録または再生する装置を制御することを備えた構成を有する。

【0022】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【0023】(コンテンツの配信)公開のネットワークを介してコンテンツを配信するコンテンツ送受信システムについて説明する。図1はコンテンツを送受信するシステム図である。

【0024】図1において、100はコンテンツの配信側である放送発信局、101は契約により放送発信局100からの情報を受信およびメディアへの記録または再生可能なユーザ側の受信記録再生装置、102は契約することで発行されるカード、103は公開上のネットワーク、104はテレビ、105はカード102から他の装置へのデータの送受信を行うためのインターフェースの通信ケーブルである。

【0025】放送発信局100から発信されるコンテンツとしては、映画などのビデオ、ジャズなどのオーディオ、ゲーム、著作物などの文字情報等であり、伝送コンテンツは暗号化されている。

【0026】本実施の形態では、コンテンツはMPEG2(ISO 13818-2)の伝送フォーマットであるトランスポートストリームを用いて伝送するビデオとして説明する。

【0027】このコンテンツ送受信は、放送発信局100からコンテンツを暗号化してネットワーク103を介してユーザの受信記録再生装置101に伝送され、受信記録再生装置101で復号することでテレビ104に再生する。

【0028】コンテンツを暗号化する方式としては、同じ鍵データを有する共通鍵暗号方式とし、この場合、ユーザが受信契約することで発行されたカード102と放送発信局100に共通鍵(マスタ鍵)を有することにより、図2のように行うものとする。

【0029】まず、送信側では、配信するコンテンツを

暗号化するためのコンテンツ鍵108を生成し、コンテンツ鍵108を用いて暗号部107によりコンテンツを暗号化したコンテンツ情報とコンテンツ鍵108をマスタ鍵109を用いて暗号部107により暗号化したコンテンツ鍵情報を受信側にネットワーク106を介して伝送する。

【0030】受信側では、暗号化したコンテンツ鍵情報を、マスタ鍵111を用いて復号部110により復号化してコンテンツ鍵112とし、暗号化したコンテンツ情報を、コンテンツ鍵112を用いて復号化することでコンテンツが暗号化伝送される。

【0031】伝送されるコンテンツはタイトル毎に所定の単位で分割して図3に示す様に行われるものとする。図3はコンテンツを伝送するフォーマットを示す図である。

【0032】図3において、113はフォーマットの先頭を示すプリアンプル、114はコンテンツの送信先を示す送信先アドレス、115はコンテンツの送信元を示す送信元アドレス、116は送信データであるデータ部であり、117はタイトル等のデータを配置したヘッダ情報部、118はコンテンツを復号するためのコンテンツ鍵である復号鍵情報部、119はコンテンツ情報から構成されたコンテンツ情報部である。ここで、ヘッダ情報部117はタイトル単位で同一情報とする。

【0033】(コンテンツのメディアへの記録)放送発信局100からのコンテンツを受信記録再生装置101への記録動作について説明する。図4はカード102における構成図である。

【0034】図4において、200は受信記録再生装置101とデータの送受信を行うためのカードI/O、201はカード102を制御するCPU、202はCPU201が実行するプログラムを記憶しているROM、203は放送発信局100から配信されるコンテンツに用いられる暗号アルゴリズムを備えた暗号部α、204は乱数を発生する乱数発生器、205は受信記録再生装置101の外部装置とデータの送受信を行うインターフェース、206は配信されたコンテンツをメディア等に記\*

\*録する場合に用いられる暗号アルゴリズムを備えた暗号部β、207は放送発信局から配信された暗号化したコンテンツを復号するための鍵であるマスタ鍵、208はコンテンツの再生に必要な情報を記憶する不揮発性メモリで構成された管理情報部、209は後述する再生課金の処理に用いられる不揮発性メモリで構成された再生課金テーブル部である。

【0035】図5は受信記録再生装置101における構成図であり、図5において、210は公開上のネットワーク103を介して放送発信局100とデータの送受信を行うためのネットワークインターフェース、211はMPEGのビデオ、オーディオのデータを復号する伸長処理部、212はカード102とデータの送受信を行うためのカードI/O、213は記録フォーマットを作成する信号処理部、214はレーザ駆動部、215は光ヘッド部、216はディスク、217は受信記録再生装置101を制御するCPU218はユーザが受信記録再生装置101の動作を設定する設定部218である。

【0036】ここで、カード102はカードI/O200と受信記録再生装置101のカードI/O211で通信できる様に受信装置101に配置する。

【0037】表1は管理情報部208における記憶データのフォーマットで、300はコンテンツのタイトル、301はコンテンツ毎の識別を行う識別コード、302はコンテンツを暗号化して記録する場合における鍵、303はコンテンツを外部に出力する場合にその回数を制限する複写回数制限コード、304はコンテンツ毎のメディアに記録した時における再生課金するための料金を識別する等級コード、305はコンテンツ毎の記録した時における日付を示す日付コード、306はメディアに記録したコンテンツの再生装置外部への出力における品位を制約する再生制約コード、307はコンテンツを記録する場合にコンテンツ毎の配信源を記録するトレースコード、308は再生課金した場合の課金料金である。

【0038】

【表1】

300	301	302	303	304	305	306	307	308
タイトル	識別コード	鍵	複写回数制限コード	等級コード	日付コード	再生制約コード	トレースコード	課金料金
X . .	B . .	A . .	2 . .	T1	1999.4	011		

【0039】タイトルXのコンテンツを受信記録再生装置101へ記録する動作について説明する。まず、放送発信局100からネットワーク103を介して暗号化した形式で伝送したコンテンツは、受信記録再生装置101のネットワークインターフェース210で受信し、カ

ードI/O212よりカード102に伝送する。

【0040】カード102ではROM202の制御プログラムをCPU201が実行することで図6に示す様にステップS11では乱数部204において第1の乱数を発生し鍵Aとし、ステップS12では乱数部204にお

いて第2の乱数を発生し乱数Aとし、ステップS13では乱数Aと管理情報部208に識別コードとして登録されている情報を比較し、一致した場合（no）はステップS12を実行し、不一致した場合（yes）はステップS14において乱数Aを識別コードBとする。これにより後述する記録時にコンテンツを暗号化するための鍵と再生時にそのコンテンツの復号に必要なカード102に記憶した鍵を識別可能とする識別コードのペアを作成する。

【0041】そして、カードI/O200を介して入力したコンテンツを所定の単位でマスタ鍵207を用いて暗号部α203により復号化し、そのコンテンツを、鍵Aを用いて暗号部β206により暗号化し、識別コードBと暗号化したコンテンツをカードI/O200から受信記録再生装置101に送信し、かつ鍵Aと識別コードBと詳細は後述するが、ヘッダ情報部117に含まれる情報を管理情報部208にタイトル単位で表1の様に記憶する。ここで、設定がなければ0として以降説明する。

【0042】受信記録再生装置101はカードI/O212で受信した識別コードとコンテンツを信号処理部213においてエラーを訂正するためのエラー訂正コードを付加し記録フォーマットに変換し、その記録情報をレーザ駆動部214において電気信号を光学信号に変換するための処理を行い、光ヘッド部215によりディスク216に記録する。

【0043】以上の動作によりネットワークを介したコンテンツの配信に用いる暗号アルゴリズムとメディアへの記録または再生可能な装置に用いる暗号アルゴリズムを異なる様にすることで、ネットワークに用いる暗号アルゴリズムが解読されてもメディアに暗号化して記録しているコンテンツの復号は不可能であり、コンテンツに著作権保護の安全性が強固となる。

【0044】また、カード内でコンテンツの暗号を変換することで、変換過程の平文を外部に公開することなくコンテンツのセキュリティが保たれたまま暗号の変換ができる。

【0045】（メディアからのコンテンツ再生）受信記録再生装置101に記録しているタイトルXのコンテンツの再生について説明する。まず、受信記録再生装置101はディスク216からタイトルXのコンテンツと識別コードBを光ヘッド部215より光学的に読み出した情報をレーザ駆動部214において電気信号に変換し、信号処理部213においてエラー訂正を行い、カードI/O212より識別コードBとコンテンツをカード102に送信する。

【0046】カード102ではROM202の制御プログラムをCPU201が実行することでカードI/O200よりコンテンツと識別コードBを入力し、識別コードBを管理情報部208に記録されている識別コードと

比較し、一致した場合には一致した識別コードにおける鍵（A）を用いて暗号部β206によりコンテンツを復号化してカードI/O200より受信記録再生装置101に送信する。

【0047】受信記録再生装置101ではカードI/O212より受信したコンテンツを伸長処理部211でMP EG処理を行い、ビデオまたはオーディオを出力する。

【0048】以上の動作により暗号化してコンテンツをメディアに記録した場合に、コンテンツに鍵情報をメディアに記録せず独特な（識別コード）コードを記録し、識別して再生可能にすることで、鍵をカード外部に公開することなく復号可能となり、著作権を強固にすることができる。

【0049】以降再生動作におけるカード102の動作について説明する。

【0050】（他のメディアへのデジタル出力の回数制限）受信記録再生装置101のディスク216から再生したコンテンツを、図7にある様にカード102のインターフェース205から通信ケーブル105を介して接続した外部装置である記録装置106へのコンテンツのデジタル出力の制限について説明する。

【0051】ここで、前記表1の複写回数制限コードは、データを設定しない場合は0とし、設定した場合においてデジタル出力するごとにカウントダウンして1となった場合にデジタル出力不許可とするものとし、例えば1回だけデジタル出力を許可する場合は2を設定するものとし、受信記録再生装置101の設定部218より外部装置である記録装置106へのコピー動作を設定した場合におけるカード102の動作を説明する。

【0052】ステップS21では複写回数制限コードと0を比較し、一致した場合（no）はステップS24を実行し、不一致の場合（yes）はステップS22において複写回数制限コードと1を比較し、一致した場合

（no）はインターフェース205からコンテンツの出力を行わずに終了し、不一致の場合（yes）はステップS23において複写回数制限コード-1を行い、ステップS24においてインターフェース205からコンテンツを出力する。

【0053】例えばタイトルXでは、複写回数制限コードが2であることから1度だけ外部への出力が可能である。

【0054】以上の様に、カード内部でインターフェースとインターフェースから外部へのコンテンツのコピー等の出力回数を制限できる情報をタイトル毎に備えることで、カード外部に情報が漏れることなく容易にインターフェースからのコンテンツ情報の出力を止めることができるため記録したコンテンツの著作権保護が強固となる。

【0055】（再生課金）メディアに記録したコンテン

ツを再生する毎に料金を徴収するための再生課金について説明する。

\* 記憶データのフォーマットである。

【0057】

【0056】表2は再生課金テーブル部209における\*

【表2】

等級部 400	日付部 401	転送部 402	料金部 403	
T1	1999.6	T10	\$10	メインテーブル領域 404
T2	1999.6	T11	\$8	
T3	1999.6	T15	\$6	
⋮	⋮	⋮	⋮	
T10	1999.5	T3	\$9	転送テーブル領域 405
T11	1999.4	T15	\$7	
⋮	⋮	⋮	⋮	

【0058】表2において、400はコンテンツの料金を識別するためのコードである等級部、401は等級部400の各情報の日付を示す日付部、402は料金検索における番地を示す転送部、403は再生課金の料金を示す料金部、404は再生課金における基本料金を示すメインテーブル領域、405は基本料金以外の料金を示す転送テーブル領域である。

【0059】ここで、日付コード305および日付部401における日付情報は（西暦、月）で表示するものと、再生課金の料金を確定する際、転送部402が示す等級部400のコードが転送テーブル領域405からメインテーブル領域404へ検索動作が移動した場合には、その等級部400のコードにおける料金部403の料金を無条件に課金するものとする。

【0060】ステップS31では、再生するコンテンツの等級コード304をメインテーブル404における等級部400のコードと比較し、不一致の場合（no）は再生を終了し、一致した場合（yes）は一致したコードの情報を参照し、ステップS32を実行する。

【0061】ステップS32において、一致した等級部400のコードにおける日付部401とコンテンツの日付コード305の日付情報を比較し、日付コード305≧日付部401の場合（yes）は、ステップS35において料金確定として料金部403における該コンテンツの料金を課金料金308に加算し、日付コード305<日付部401つまり日付コード305が古い場合（no）は、ステップS33において該等級部400のコードにおける転送部402が示す転送テーブル領域404における等級部400のコードにおける日付部401と該コンテンツの日付コード305を比較する。

【0062】ステップS33において、日付コード305≧日付部401の場合（yes）はステップS35において料金確定として料金部403における該コンテンツの料金を課金料金308に加算し、日付コード305<日付部401つまり日付コード305が古い場合（no）はステップS34を実行する。

【0063】ステップS34において、該転送部402におけるコードとメインテーブル領域404の最終コード（T9）とを比較し、メインテーブル領域404以内のコードであれば、ステップS35において、料金確定として料金部403における該コンテンツの料金を課金料金308に加算し、以外のコードであれば、転送テーブル領域405においてステップS33を実行する。

【0064】例えば、タイトルXを再生する場合は、ステップS31において等級コード304がT1なので等級部400のT1における情報を参照し、ステップS32においてタイトルXの日付コード305と等級部400のT1における日付部401の日付情報を比較し、日付コード305が古いことから、ステップS33において転送部402が示す転送テーブル領域405における等級部400のT10の日付部401とタイトルXの日付コード305における日付情報を比較し、日付コード305が古いことからステップS34において転送部402が示す等級部300のコードがメインテーブル領域404を示すかを確認し、転送部402はT3であることからメインテーブル領域404なので、ステップS35において等級部400のT3における料金部403を課金料金308に加算し、タイトルXの再生課金を行う。

【0065】そして、定期的に受信記録再生装置が課金料金308を放送発信局100に送信することで、後で放送発信局100は課金料金308を基に銀行口座等から課金料金を引き落とす。

【0066】メディアにコンテンツを記録した場合における料金のリンクを示す等級コードと日付けを示す日付コードをカードに記憶しておき、放送発信局100から定期的に配信される課金データ情報を再生課金テーブル部209に有する様にし、再生する際に上記動作をすることによりコンテンツの再生課金を行うことで、コンテンツは時が進むにつれ社会的価値（時価）が変わることから、メディアに記録したコンテンツを再生した時の時価で再生課金することができる。

【0067】(再生制約の動作) メディアに記録したコンテンツを別の装置(メディア)に出力する場合に、そのコンテンツの視聴条件の制約について説明する。

【0068】表3はコンテンツの制約情報であり、この\*

\* 情報の内容をROM202に有するものとする。

【0069】

【表3】

コード	制約
<b>ビデオ</b>	
001	SDをサブサンプリング(間引き)する。
010	プログレッシブ(ノンインターレス)をインターレスにする。
011	HDをSD以下にダウンコンバートする。
<b>オーディオ</b>	
101	ダウンサンプリングする。(48kHz系→16kHz、44.1kHz系→13.7kHz)
110	チャンネル(ch)制限する。(2chの有効(5.1ch→2ch))
111	上記101、110を共に行う。

【0070】ステップS41では再生するコンテンツの再生制約コード306と0を比較し、一致した場合(n o)は再生するコンテンツへの制約は無しとし、不一致の場合(y e s)は制約情報が有るものとしてステップS42において再生制約コード306に応じてROM202に有る制約情報の内容を実行する。

【0071】例えば、タイトルXであれば、再生制約コード306が011なので、CPU201において高細精なハイビジョン(HD)のビデオデータの走査線数を現行テレビ放送(NTSC)レベルまで操作(減少)してから、インターフェース205から通信ケーブル105を介して出力する。

【0072】メディアに記録したコンテンツの再生制約の条件を示す再生制約コードをカードに記憶しておき、外部の装置にインターフェースを介してコンテンツを出力する際に上記動作をすることで、仮にコピーしたとしてもオリジナルとの品質における差別化が可能であり、オリジナルの価値の低下を防ぐことができる。

【0073】(トレース動作) メディアに記録したコンテンツの発信源の送信元アドレス115をカードに記録しておくことで、ネットワーク103を介して不正コピーされたコンテンツを記録した場合にその発信源が特定できる。

【0074】

【発明の効果】以上のように本発明によれば、下記の特徴を備えたカードを用いることで、メディア等に記憶したコンテンツの著作権保護が強固となる。

【0075】(1) ネットワークを介したコンテンツの配信に用いる暗号アルゴリズムとメディアへの記録または再生可能な装置に用いる暗号アルゴリズムを異なるようにすることで、ネットワークに用いる暗号アルゴリズムが解読されても、メディアに暗号化して記録しているコンテンツの復号は不可能であり、コンテンツに著作権保護の安全性が強固となる。

【0076】また、カード内でコンテンツの暗号を変換することで、変換過程の平文を外部に公開することなく、コンテンツのセキュリティが保たれたまま暗号の変換ができる。

【0077】(2) コンテンツは時が進むにつれ社会的

価値(時価)が変わるため、メディアに記録したコンテンツを再生した時の時価で再生課金することができる。

【0078】(3) 暗号化してコンテンツをメディアに記録する場合に、コンテンツに鍵情報をメディアに記録せず、独特なコードを記録し識別して再生可能にすることで、鍵をカード外部に公開することなく復号可能となり、著作権を強固にすることができる。

【0079】(4) カードにインターフェースとコンテンツ毎の出力回数を制限する情報を保持することで、カード自身が不正コピーの検出し、阻止することができる。

【0080】(5) ネットワークを介してコンテンツを記録する場合に、そのコンテンツの発信源であるアドレスを保持することで、不正コピーが流通した場合に、その発信源が特定できる。

【0081】(6) デジタル出力するコンテンツの視聴条件を制約する情報を保持し、制約情報に応じてデジタル出力するコンテンツの品質を制約することで、仮にコピーしたとしても、オリジナルとの品質における差別化が可能であり、オリジナルの価値の低下を防ぐことができる。

【図面の簡単な説明】

【図1】本発明の一実施例における伝送システムの構成図

【図2】同伝送システムにおけるコンテンツの暗号化伝送構成を示すブロック図

【図3】同伝送システムの伝送フォーマット構成図

【図4】同伝送システムに用いられるカードの構成図

【図5】同伝送システムの受信記録再生装置の構成図

【図6】同識別コード生成におけるフローチャート

【図7】本実施例における他の伝送システムの構成図

【図8】本実施例の記録コンテンツの出力の制限におけるフローチャート

【図9】本実施例の再生課金におけるフローチャート

【図10】本実施例の記録コンテンツの出力における制約を検出するフローチャート

【符号の説明】

100 放送発信局

101 受信記録再生装置

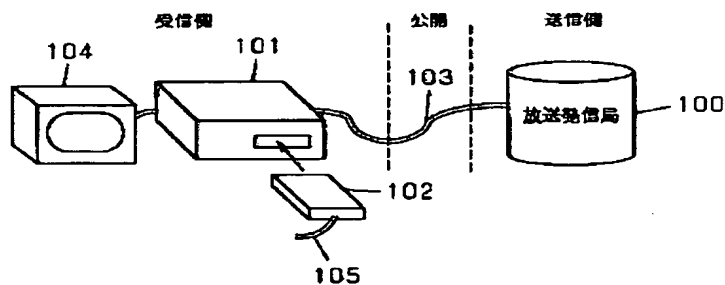


102 カード  
 103 ネットワーク  
 104 テレビ  
 105 通信ケーブル  
 106 記録装置  
 200 カードI/O  
 201 CPU  
 202 ROM  
 203 暗号部α  
 204 乱数部  
 205 インターフェース  
 206 暗号部β  
 207 マスタ鍵  
 208 管理情報部  
 209 再生課金テーブル部  
 210 ネットワークインターフェース  
 211 伸長処理部  
 212 カードI/O  
 213 信号処理部  
 214 レーザ駆動部

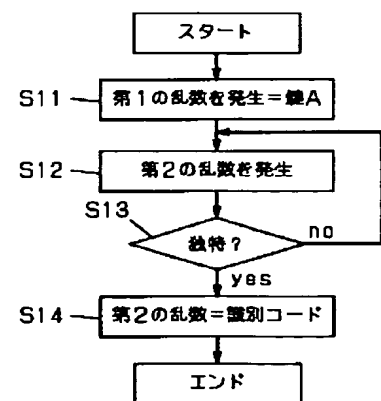
\*215 光ヘッド部  
 216 ディスク  
 217 CPU  
 218 設定部  
 300 タイトル  
 301 識別コード  
 302 鍵  
 303 複写回数制限コード  
 304 等級コード  
 10 305 日付コード  
 306 再生制約コード  
 307 トレースコード  
 308 課金料金  
 400 等級部  
 401 日付部  
 402 転送部  
 403 料金部  
 404 メインテーブル領域  
 405 転送テーブル領域

\*20

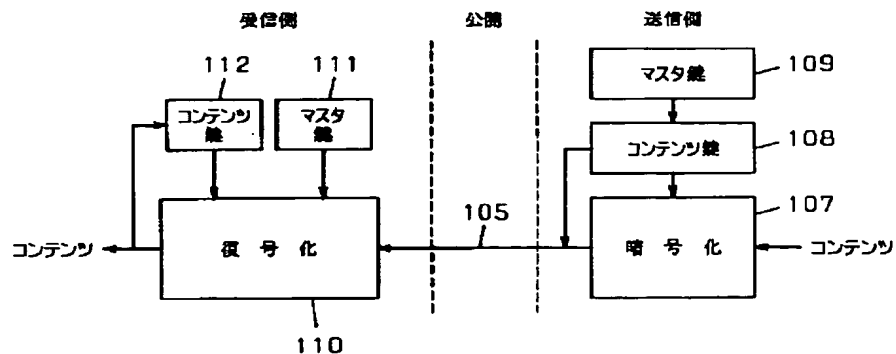
【図1】



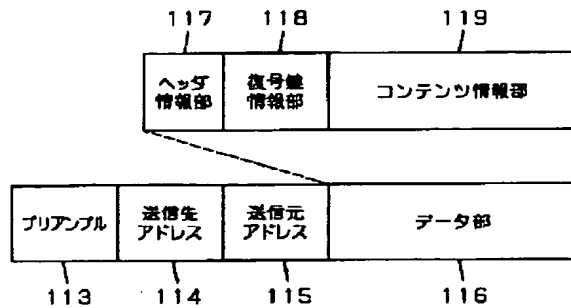
【図6】



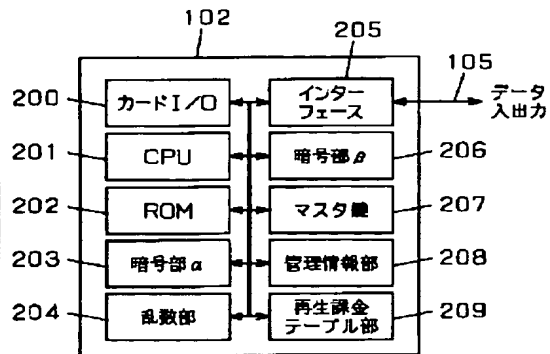
【図2】



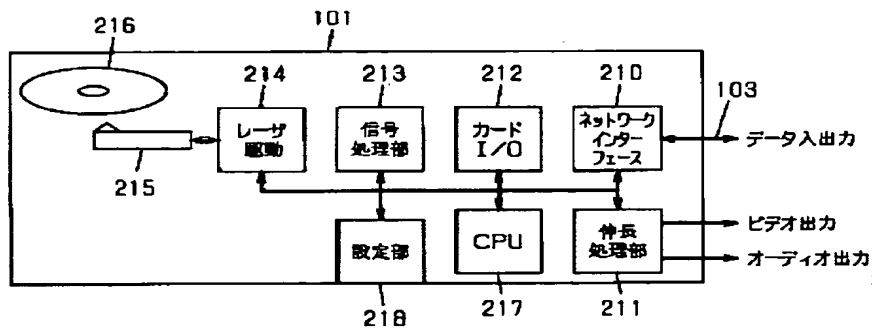
【図3】



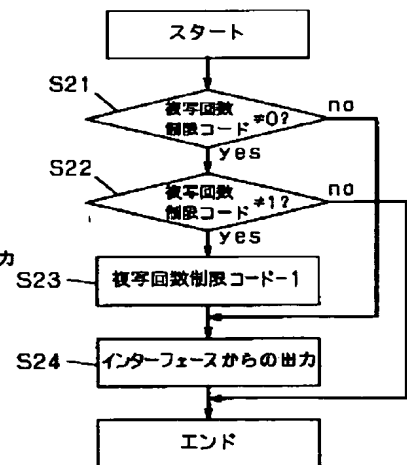
【図4】



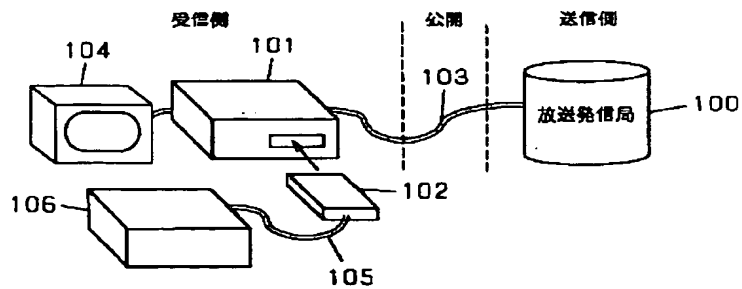
【図5】



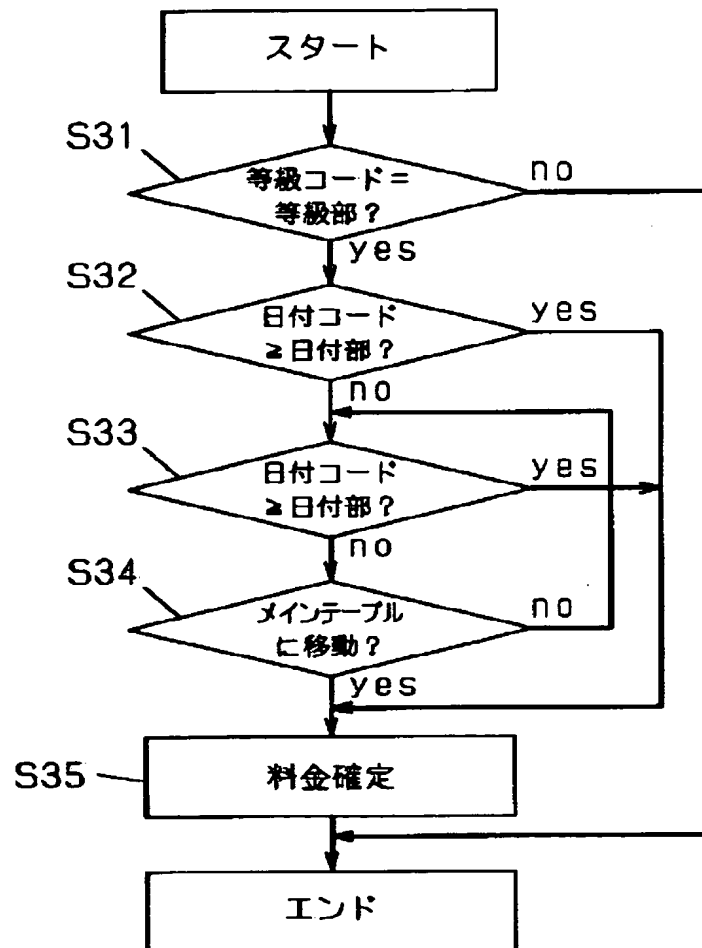
【図8】



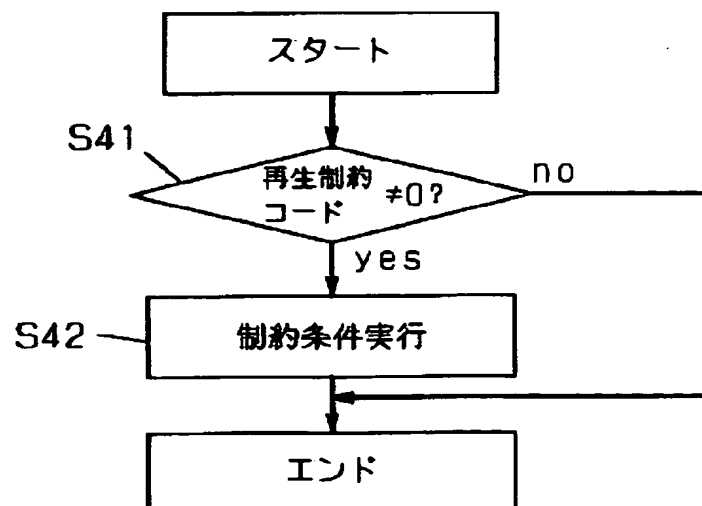
【図7】



【図9】



【図10】



フロントページの続き

F ターム(参考) 5B035 BB09 BC00 CA08 CA11  
5B085 AE12 AE29  
5C064 CA14 CB08 CC04  
5J104 AA01 AA07 AA12 AA16 AA34  
AA41 EA04 EA08 EA16 EA22  
JA03 KA01 KA02 NA02 NA35  
NA36 NA37 NA40 PA06 PA11